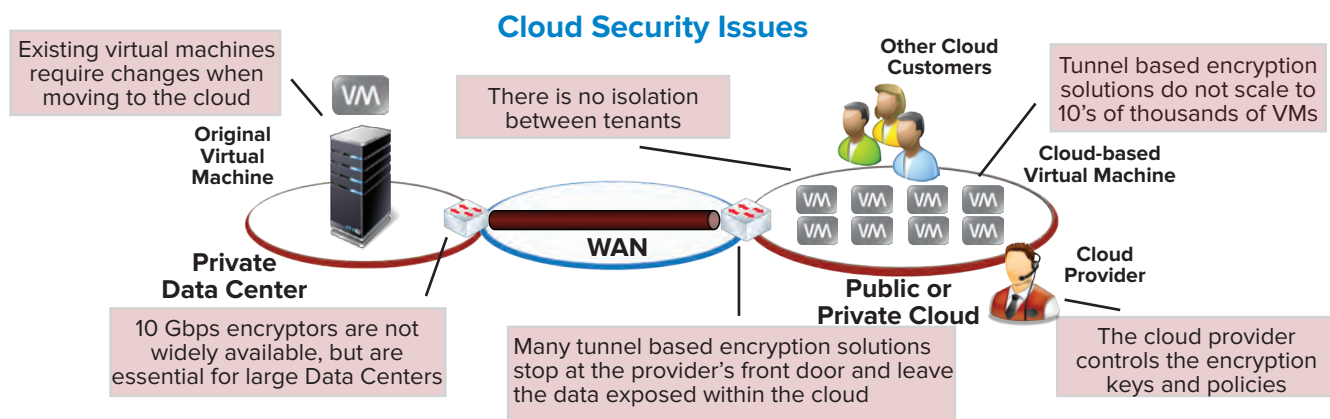


## Making the Cloud Safe for Sensitive Workloads

The cloud provides a compelling case for cost savings, agility and operational efficiency that cannot be ignored. Executing IaaS (Infrastructure as a Service) workloads while protecting sensitive information has been challenging if not impossible in the past, but Certes Networks has developed a new solution to keep sensitive information secure in cloud environments.

The characteristics of cloud environments typically include the terms “scalable”, “dynamic” and “elastic” – terms that are nearly opposite of the user experience with IPsec tunnels established with IKE (the predominant method of securing connections to virtualized private data centers and public cloud infrastructures). The IKE/IPsec method also leaves control of the policies and keys with the provider, which may or may not be desired by the provider or client, and is nearly always incompatible with data privacy regulations. Furthermore, tunnels force point-to-point connectivity that is limited to two endpoints per tunnel. This point-to-point mapping of large-scale distributed networks is exponentially complex to the point of being prohibitive in terms of both the cost to manage and the performance limitations it imposes.

These and other critical cloud security issues are illustrated in the diagram below.



## The Virtual CEP (vCEP) Powered by Certes TrustNet Manager™

Building upon our groundbreaking solutions for wide area network and data center encryption, Certes Networks has developed the Virtual Certes Enforcement Point (vCEP). Powered by Certes TrustNet Manager™, this solution allows customers to extend the benefits of tunnel-less group encryption to virtualized data centers and public/private clouds. In doing so, we have provided a means for organizations to reduce data center costs while maintaining high standards for protecting sensitive information for compliance and risk reduction.

### Certes Networks' vCEP

#### Virtualized software-based encryption appliance

- It's a VM - and behaves like one

#### Runs as a VM on VMWare hypervisor

- Requires no changes to the Tenant VM

#### Encrypts network traffic

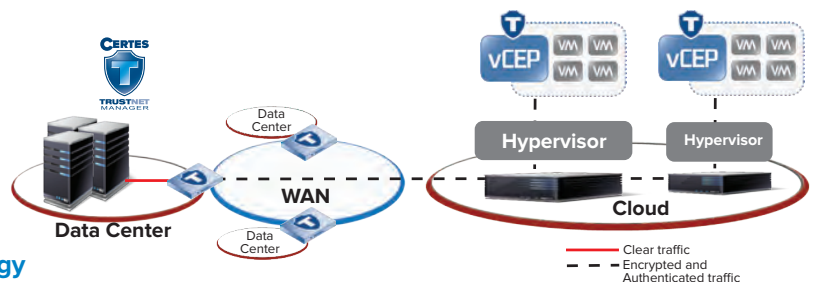
- From data center to cloud across the WAN
- From server to server in the cloud

#### Proven Certes Networks Group Encryption technology

- Interoperable with physical CEP

#### Flexible multi-layer encryption

- Securely connect to the cloud via low-cost Layer 2 Ethernet
- Extend existing data center networks to the cloud



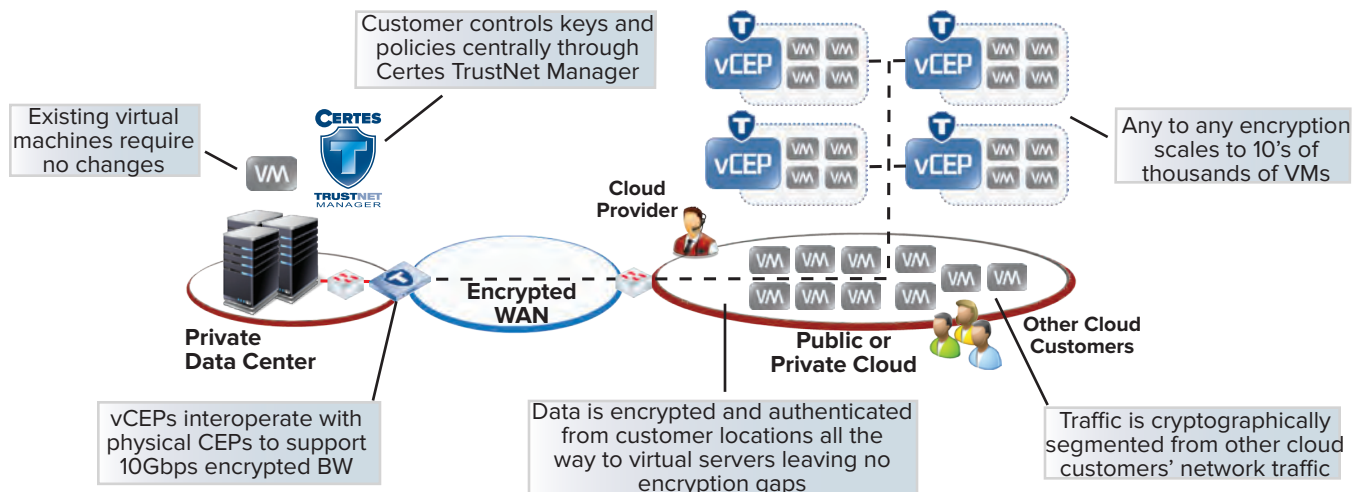
Powered by TrustNet Manager, this solution provides performance, independent scalability and reliability, and allows cloud customers to maintain control of keys and policies.

## Cloud Security with vCEP and Certes TrustNet Manager

Using the vCEP in conjunction with TrustNet Manager, organizations can take advantage of all of the benefits of private or virtualized data centers and IaaS clouds without compromising on their security or performance. Easy drag and drop policy definitions, role based access control and automated key rotation make security an integral part of your cloud deployment without imposing performance, reliability or visibility restrictions.

Benefits include:

- **Secure Connectivity** - Encrypts traffic from private data centers to the cloud and among VMs running in the cloud without encryption gaps. Allows any-to-any connectivity among all participants without using point-to-point tunnels
- **Cryptographic Isolation** - Protects the VM and the data center from threats originating in the public cloud
- **Distributed Performance** - Distributes the load of encrypting traffic across each newly migrated VM to the server on which it's running in order to take advantage of the massive scalability and elasticity of the cloud
- **High Bandwidth and Low Latency** - In concert with the physical CEP VSE family, encrypts up to 10Gbps with low latency
- **Customer Control** - Allows cloud users to maintain control of their own policies and keys
- **Flexibility** - Takes advantage of the best options for network connectivity and cloud environments
- **Compliance** - Comply with regulatory requirements to protect sensitive information in shared environments



## Group Keying - The Key to Cloud Security

The technology that enables these essential solution components has been proven over nearly ten years of deployments to government agencies, defense contractors, financial organizations, as well as enterprises looking to secure PCI, HIPAA and other compliance-driven privacy requirements.

Certes Networks is building on these proven technologies to provide a solution that makes the cloud safe for sensitive workloads. This will lead to secure and optimized solution architectures for data centers and cloud environments that dramatically reduce IT costs while improving agility.